REMARKS

[0003] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. Claims 1-2, 6-9, 11, 22-24, 28, 31-32, 43, and 46-47 are presently pending. Claims amended herein are 1, 6, 22, 31, and 43. Claims withdrawn or cancelled herein are 3-5, 10, 12-21, 25-27, 29-30, 33-42, 44-45, and 43. New claims added herein are none.

Statement of Substance of Interview

[0004] The Examiner graciously talked with me—the undersigned representative for the Applicant—on June 20, 2007. Applicant greatly appreciates the Examiner's willingness to talk. Such willingness is invaluable to both of us in our common goal of an expedited prosecution of this patent application.

[0005] During the interview, Examiner and I discussed the new-matter based rejections and the type of evidence needed to overcome that rejection. Consequently, Applicant will be submitting forthwith this response a declaration from Min Feng, who is at least one of ordinary skill in the art. That declaration will explain why the changes to the specification are not actually "new matter."

Formal Request for an Interview

[0006] If the Examiner's reply to this communication is anything other than allowance of all pending claims, then I formally request an interview with the Examiner. I encourage the Examiner to call me—the undersigned representative

for the Applicant—so that we can talk about this matter so as to resolve any outstanding issues quickly and efficiently over the phone.

[0007] Please contact me or my assistant to schedule a date and time for a telephone interview that is most convenient for both of us. While email works great for us, I welcome your call to either of us as well. Our contact information may be found on the last page of this response.

Claim Amendments and Additions

[0008] Without conceding the propriety of the rejections herein and in the interest of expediting prosecution, Applicant amends claims 1, 6, 22, 31, and 43 herein.

§ 132 Declaration

[0009] Forthwith this response, Applicant will be submitting a declaration from Min Feng, who is at least one of ordinary skill in the art. That declaration will explain why the changes to the specification are not actually "new matter."

[0010] In the interim while the signed declaration is in transit to the Office, a copy of Exhibit A of the declaration is provided herewith. That Exhibit includes the bulk of the explanation of why the changes (labeled "A" through "E") are not actually new matter.

[0011] The primary reason why the changes are not new matter is because each of the identified changes are fixed problems or errors that would have been apparent to one of ordinary skill in the art. Furthermore, some changes

represent equivalent ways of saying the same thing, but the change presented the same information in a more clear manner.

Formal Matters

[0012] This section addresses any formal matters (e.g., objections) raised by the Examiner.

IDS

[0013] The Examiner indicated that the 4th citation in the IDS filed 14 October 2003 was not found in the file wrapper and not considered. Accordingly, Applicant submits a copy herewith.

Specification

[0014] The Examiner objects to the amendment to the specification filed 25 November 2003 because it introduces new matter into the disclosure. Applicant disagrees with this assessment of the specification amendment.

[0015] Forthwith this response, Applicant will be submitting a declaration from Min Feng, who is at least one of ordinary skill in the art. That declaration will explain why the changes to the specification are not actually "new matter."

Substantive Matters

Claim Rejections under § 112

[0016] Claims 5, 6, 27, and 48 are rejected under 35 U.S.C. § 112, 1st ¶, for failing to comply with the written description requirement. In light of the § 132 declaration showing that the changes to the specification are not new matter, Applicant submits that these rejections are not applicable anymore. Accordingly, Applicant asks the Examiner to withdraw these rejections.

Allowable Subject Matter

[0017] **Claim 33**: The examiner indicated that objected-to dependent claim 33 would be allowable if rewritten in independent form—including all of the limitations of the base claim and any intervening claims.

[0018] Applicant has done just that. Herein, the subject matter of claim 33 has been moved upto and included within independent claim 31. Accordingly, Applicant asks that this objection be withdrawn and claim 31 be recognized as allowable

[0019] **Claims 5, 6, 27, and 48**: The examiner indicated that these claims would be allowable if rewritten to overcome the rejection under § 112, 1¶, set forth in this Action and to all of the limitations of the base claim and any intervening claims.

[0020] The soon-to-be submitted declaration will show that there is no new matter in the amendment to the specification provided in the "Preliminary

Amendment." Consequently, these claims are allowable. Since these claims are dependent claims, Applicant amends their base claims to incorporate the subject matter of the allowed claims.

[0021] More particularly, the subject matter of claim 5 is moved into claim 1; claim 6 is now independent and includes the subject matter of claim 1; the subject matter of claim 27 is now included in independent claim 22; and the subject matter of claim 48 is now included in independent claim 43.

[0022] Accordingly, Applicant asks that this objection be withdrawn and claim 31 be recognized as allowable

[0023] Furthermore, all remaining dependent claims depend from one of these independent claims that now include allowable subject matter. Consequently, Applicant submits that all dependent claims are allowable because they depend from allowable claims.

Claim Rejections under §§ 102 and 103

[0024] In light of the amendments presented herein and the forthwith submitted declaration (explaining how the previously submitted specification amendments did not constitute new matter), Applicant submits that the claim rejections under 35 U.S.C. §§ 102 and 103 are moot. Accordingly, Applicant asks the Examiner to withdraw these rejections.

Dependent Claims

[0025] In addition to its own merits, each dependent claim is allowable for the same reasons that its base claim is allowable. Applicant requests that the Examiner withdraw the rejection of each dependent claim where its base claim is allowable.

Conclusion

[0026] All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the **Examiner is urged to contact me before issuing a subsequent Action**. Please call/email me or my assistant at your convenience.

Respectfully Submitted,

Dated: 10-8-07

By: _____

Kasey C. Christie
Reg. No. 40559
(509) 324-9256 x232
kasey@leehayes.com
www.leehayes.com

My Assistant: Carly Bokarica
(509) 324-9256 x264
carly@leehayes.com

Hi, Kasey

Here are my comments about Bin's patent's change from A to E. Please see the comments injected among change descriptions.

Best Regards!

Min FENG
Tel: +86(10)58963453
Internet Media Group
Microsoft Research Asia

Exhibit A

From: Kasey Christie
Sent: Monday, August 06, 2007 9:00 AM
To: 'Min FENG'
Cc: PLaw; Carly Bokarica
Subject: MS#306096.01 MS1-1753US | Seeking expert advice

Min:

Thank you for your help. In order to prepare for that declaration, can I get you to explain each of the changes? I will list each one below. There are 5 of them (changes A-E).

Please mark your in-line comments with preceeding "[Min]"

Note that the ~~crossed-out text~~ represents deletions and underlined text represents additions.

Change A

[0050] The content publisher generates the sharing polynomial $f(x)$ ~~over a finite field Z_N~~ where $a_o = SK$. Although polynomial interpolation is described, other collections of functions may also be utilized. Each partial secret share S_i may then be calculated using Equation (3), which is shown as follows:

$$S_i = f(id_i) \bmod N \; \phi(N), \qquad (3)$$

where N is an RSA modulus and $\phi(N)$ is an Euler totient function.

[Min] For the part 2: According to number theory, for any arbitrary integer α between 1 and N-1, $\alpha^{\Phi(N)} = 1 \bmod N$. So any operations such as addition, subtraction, multiplication and division on the exponent position should mod $\Phi(N)$ instead of N. The result of $f(x)$ is used on the exponent position of the operation $a^{x} \bmod N$, so the result of the polynomial $f(x)$ should mod $\Phi(N)$.

For the part 1: First since N is a compound number, Zn is definitely not a finite field. So any operations such as addition, subtraction, multiplication and division on the exponent position should mod $\Phi(N)$. $f(x)$ can be said that it is defined over Z_n^* not Zn, but any polynomial in $Z[x]$

(coefficients are in Z) can be regarded as a polynomial in $Z_n^*[x]$ by mapping the coefficients $a_i \rightarrow a_i \bmod \phi(N)$.

These errors can be detected and corrected by any one learn some number theory. They are some kind of typo. The changes are correct.

Change B

[0053] At block 514, for instance, the content publisher may broadcast *k* public witnesses of the sharing polynomial's coefficients, which are denoted as $\{g^{a_0}, \cdots, g^{a_{k-1}}\}$, where $g \in Z_N$ $g \in Z_N^*$. After broadcast, the content publisher may destroy the polynomial. At block 516, each license authority id_i verifies validity of the received partial secret share. Validity may be checked by determining if Equation (4), as shown below, holds for the received partial secret share S_i utilizing the sharing polynomial's coefficients which were broadcast at block 514:

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \underline{\bmod N} \qquad (4)$$

In this way, each license authority id_i, may verify the validity of the received partial secret share S_i without exposing or knowing the secret, i.e. the private key *SK*.

[Min] For part 1: $g \in Z_n^*$ makes *g* has a large order which equals to $\phi(N)$ for the cyclic group *g* itself generates. $g \in Z_n$ can also be OK if *g* is randomly chosen from *Zn*, and has no influence on other equations and formulas. Only a small number of $g \in Z_n$ has an order less than $\phi(N)$.

For part 2: It is really good that the authors explicitly describe the equation is computed by "mod *N*". $g \in Z_n^*$ is also an element in *Zn* (Z_n^* is a subset of *Zn*). So the final result is "mod *N*". People in my field will assume the operation is "mod *N*" as default.

While these changes may not be regarded exactly as errors. The changes make the scheme more clear and solid.

Change C

[0063] At block 620, the content player, when executed by the client device, determines if *k* correct partial

licenses have been received by validating each of the partial licenses. The partial licenses may be validated as follows. First, node p calculates

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \quad \underline{\text{mod } N} \qquad ((7)$$

from the public witnesses of the sharing polynomial's coefficients, as was described in relation to block 516 of FIG. 5 and Equation (4). Equation (6) is then applied to g^{S_i} and the received partial license $prel_i$, A_1, and A_2 to calculate c. The received partial license $prel_i$ is verified by checking if the following equations hold: $g^r \cdot (g^{S_i})^c = A_1$ and $prel^r \cdot (prel_i)^c = A_2$. The above steps are repeated until the node p obtains k valid partial licenses. If k valid partial licenses cannot be obtained, generation of the formal-license fails (block 622).

[Min] It is really good that the authors explicitly describe the equation is computed by "mod N". People in my field will assume the operation is "mod N" as default. This change might not be regarded as an error. The change makes the scheme more clear.

Change D

[0064] If k valid partial licenses are obtained, then at block 624, the content player combines the partial licenses to form the formal license. For example, the node p uses the k valid partial results to calculate the formal license utilizing Equation (8):

$$license = \prod_i (prel_i)^{l_{id_i}(0)} = (prel)^{\sum_i S_i \cdot l_{id_i}(0)} \qquad ((8)$$

$$= (prel)^{SK} = ((license)^{PK})^{SK} \quad \underline{\text{mod } N,}$$

where $l_{id_i}(x) = \prod_{j=1, j \neq i}^{k} \frac{x - id_j}{id_i - id_j}$.

[Min] Again, it is really good that the authors explicitly describe the equation is computed by "mod N". People in my field will assume the operation is "mod N" as default. This change may not be regarded as an error. The change makes the scheme more clear.

Change E

[0075] At periodic intervals, for example, the license authorities may update their respective shares of the

private key *SK* through execution of the respective update module 222 of FIG. 2. At block 802, each license authority *i* generates a random *(k, m)* sharing of the secret *0* using a random update polynomial $f_{i, update}(x)$, as shown in Equation (9):

((9)

$$f_{i,update}(x) = b_{i,1}x + \_ + b_{i,k-1}x^{k-1} \bmod N$$

[Min]"mod N" is definitely wrong. Because the result of $f_{i,update}(x)$ is used as the exponent value in the operation of $a^x \bmod N$. So the result of the polynomial $f_{i,update}(x)$ should be mod $\phi(N)$. I suggest that "mod $\phi(N)$" be added explicitly at the end of Equation 9 to avoid misunderstanding.

In addition, the authors should also explicitly state in the patent application that
1) $\phi(N)$ is public
2) PK is not disclosed
The current version does not mention explicitly the above conditions in the patent application. They are implicitly used to make the whole system work. Stating them explicitly can help readers understand the equations and the whole system.

Thank you.

kasey

Kasey Christie
(509)324-9256 x232
kasey@leehayes.com

Lee & Hayes pllc, Intellectual Property Law
421 West Riverside, Suite 500, Spokane, WA 99201 | 509.323-8979 fax | www.leehayes.com